"Express Mail" mailing label number EL823499348US

APPLICATION FOR LETTERS PATENT
OF THE UNITED STATES

NAME OF INVENTORS: VASSILIOS KOUKOULIDIS
212 VIA D'ESTE #1101
DELRAY BEACH, FL 33445

GEORGE STAMATELOS
152 VIA D'ESTE #910
DELRAY BEACH, FL 33445

RICK JEZIERNY
11535 SUNDANCE LANE
BOCA RATON, FL 33428-5524

TITLE OF INVENTION: USE OF SHORT MESSAGE SERVICE (SMS) FOR SECURE TRANSACTIONS

TO WHOM IT MAY CONCERN, THE FOLLOWING IS
A SPECIFICATION OF THE AFORESAID INVENTION

USE OF SHORT MESSAGE SERVICE (SMS) FOR SECURE TRANSACTIONS

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to secure transactions. More particularly, the present invention relates to utilizing SMS technology and features for the purpose of establishing secure encrypted transactions.

Description of Related Art

In a wireless network, terminals, such as wireless telephones, may be used to communicate in a variety of ways. For example, a simple wireless telephone is used to convey speech, but more sophisticated telephones may be used to send text messages. A popular service for sending text messages utilizes terminals having the Short Messages Services (SMS) feature. The most widely used application of SMS is for wireless telephone users to send short alphanumeric messages to one another. Other SMS applications include receiving e-mail alerts, such as when a longer e-mail was received by the user or when a stock reaches a certain price.

Though popular, SMS has not been widely used for applications that require secure transactions. While the SMS feature built into many wireless telephones is useful for normal communications, secure transactions, such as credit card transactions, require a higher level of security that includes encryption.

A relatively new standard for mobile communication is the Universal Mobile Telecommunications System (UMTS). Though this system is capable of providing secure communications the system requires greater bandwidth than SMS and is not widely available at this time. While it is generally true that SMS can be implemented on UMTS systems, the disadvantages of UMTS remain. Thus UMTS is not available or not feasible for most wireless systems in use today.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide a system and method for conducting secure transactions utilizing SMS.

It is another object of the invention to provide a system and method for conducting secure transactions over networks that allow SMS messaging.

It is yet another object of the invention to provide a system and method for conducting credit card transactions utilizing SMS.

It is yet another object of the invention to provide user authorization and authentication for financial transactions conducted over an SMS service.

It is yet another object of the invention to provide user authorization and authentication for medical information conducted over an SMS service.

It is yet another object of the invention to exchange keys between two parties over an SMS service to establish a secure connection.

The invention uses applied cryptography to provide a secure conduit for the communication of sensitive information between two parties over an SMS service. For example, a credit card holder and a credit card center may establish a secure connection prior to engaging in a financial transaction.

The establishment and utilization of a secure conduit is accomplished in three phases.

In the first phase, authorization takes place by having a first party with a wireless terminal submit a message request containing the first party's public key to a second party at a center. The center responds with an authorization key that is encrypted using RSA software and the first party's public key. The wireless terminal, upon receiving the encrypted authorization key, utilizes RSA software and the first party' private key to decrypt the authorization key. Both parties now have the same authorization key, and each side can independently generate three additional keys: a key encryption key, and upstream message authentication key, and a downstream message authentication key.

In the second phase, the wireless terminal sends a request for a traffic key. The center, upon receiving and authenticating the request, sends a traffic key.

In the third phase, the desired confidential data is encrypted and exchanged in a secure communication between the wireless terminal and center.

The architecture of the network supporting this use of the SMS can be established either by having each party encrpyt/decrypt messages at it own end as described above. Alternatively, at least one intermediary can encrypt/decrypt and/or authenticate on behalf of a party, and use a dialup or other secure connection to communicate on behalf of the party it is representing.

The invention may be implemented over networks that support SMS, which is an advantage over technologies that are dependent on underlying network

technology that is not widely available. Advantageously, SMS requires lower bandwidth than many other digital means of communication.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is a diagram representing an example of the authorization phase in the establishment of a secure conduit for conveying sensitive data through an SMS service.

Fig. 1B is a flow diagram of the authorization phase of Fig. 1A.

Fig. 2A is a diagram representing an example of the authentication phase in the establishment of a secure conduit for conveying sensitive data through an SMS service.

Fig 2B is a flow diagram of the authorization phase of Fig. 2A.

Fig. 3 is a diagram representing an example of the data encryption phase, which utilizes a secure conduit for conveying sensitive data through an SMS service.

Fig. 4 is a diagram representing a preferred embodiment for a network architecture for implementing the invention.

Fig. 5 is a diagram representing another preferred embodiment for a network architecture for implementing the invention.

DETAILED DESCRIPTION

SMS services may be used to send sensitive information over a wireless network. Such sensitive information may be, by way of example only, credit card information or medical information, though other types of information may be sent. In a preferred embodiment described below, a user having credit card information utilizes the invention to conduct a credit card transaction through a wireless telephone with a credit card center.

With reference to Fig. 1A, authorization takes place between user's wireless terminal 10 and center 20, which in a preferred embodiment is a credit card center, using authorization communication 30. With reference to Fig. 1B, authorization phase flow chart 100 is shown. Wireless terminal 10 obtains or generates 105, if it does not already have one, user's public key. Wireless terminal 10 submits a message 110 requesting an authorization key. The message request includes user's public key which, in a preferred embodiment, comprises a 96 byte modulus and a 3 byte exponent, although other types of public keys may be used in other preferred embodiments. Center 20 encrypts 115 an authorization key and

responds to wireless terminal 10 by sending a message 120 with the encrypted authorization key. In a preferred embodiment, the authorization key is 8 bytes long and is encrypted using cryptographic means, such as the RSA public-key cryptosystem which is part of the BSAFE software package provided by RSA Security located in Bedford, Massachusetts and the public key contained in message 110. Wireless terminal 10, upon receiving message 120 comprising the encrypted authorization key, decrypts 125 the authorization key. In a preferred embodiment, the authorization key is decrypted utilizing cryptographic means, such as RSA software and the first party's private key. Now that both parties have the same authorization key, each party can independently generate 150 three additional matching keys: a key encryption key 152, and upstream message authentication key 154, and a downstream message authentication key 156. As described in further detail below, upstream message authentication key 154 is used to authenticate upstream requests; downstream message authentication key 156 is used to authenticate downstream replies; and key encryption key 152 is used to realize the secure transmission of yet another key (a traffic key, not shown) that will be used for data ciphering (for example, encrypting credit card information).

With reference to Fig. 2A, authentication of wireless terminal 10 takes place using authentication communication 40 with center 20. With reference to Fig. 2B, authorization phase flow chart 200 is shown. If wireless terminal 10 does not have an upstream authentication code, it obtains or generates 205 an upstream authentication code. In a preferred embodiment, the upstream authentication code is a hash-based message authentication code (HMAC) digest, which is a fixed-length string of code produced by taking a variable length input and upstream message authentication key 154. Wireless terminal 10 submits an encrypted message 210 having the upstream authentication code and requesting a traffic key.

Upon receiving message 210, center 20 uses an upstream message authentication key means, such as upstream message authentication key 154 and Secure Hash Algorithm 1 (SHA-1) developed by the National Institute of Standards and Technology, to authenticate 215 the request. If authentication 215 is successful, center 20 generates (if does not already have the traffic key) and encrypts 220 a traffic key using key encryption key 152. In a preferred embodiment, center 20 generates and encrypts 220 an 8 byte traffic key using Data

Encryption Standard (DES). In another preferred embodiment, center 20 generates and encrypts 220 a 16 byte traffic key using Advanced Encryption Standard (AES).

Center 20 generates 225 a downstream authentication code. In a preferred embodiment, the downstream authentication code is a hash-based message authentication code (HMAC) digest, which is a fixed-length string of code produced by taking a variable length input and downstream message authentication key 156. Center 20 sends 230 a message (which, in a preferred embodiment, contains the HMAC digest of center 20) containing the encrypted traffic key back to wireless terminal 10.

After receiving the message from center 20 containing the encrypted traffic key, wireless terminal 10 authenticates 235 the message using downstream message authentication key 156, and decrypts 240 the traffic key in the message using key encryption key 152.

With reference to Fig. 3 secure information can now be exchanged between wireless terminal 10 and center 20 using a conduit for secure encrypted communication 50 that has been established through the first two phases described above. In a preferred embodiment, the traffic key and a symmetric encryption algorithm, such as DES or AES by way of example, is employed for the actual data encryption/decryption. It should be noted that generally the longer the length of the key(s) being employed, the more difficult it is for unauthorized persons to compromise the security of the scheme (AES for example offers 128, 192 or 256 bits cryptographic keys, whereas the older DES offers 40 or 56 bits options for key lengths). The limits on the length of SMS service messages, however, may introduce limitations on key length. Nevertheless, the availability of concatenation of SMS messages (as described in (3rd Generation Partnership Project technical specification (3GPP TS) 23.040 V5.1.0 section 9.2.3.24.1, available at http://www.3gpp.org and incorporated herein by reference) may be used to allow exchanges of increased length keys.

The invention is implemented in a wireless network scenario. With reference to Fig. 4, in a preferred embodiment authorization communication 30, authentication communication 40, and secure encrypted communication 50 take place over conduit 400. Wireless terminal 10 sends and receives wireless signals to/from base transceiver station (or base station) 430, which communicates with base station controller 440. Base station controller 440 communicates with mobile

switch center 450, which communicates with SMS message center 460. Message center 460 communicates with center 20, which is a credit card center. The method by which wireless terminal 10 communicates with base transceiver station 430, base transceiver station 430 communicates with base station controller 440, base station controller 440 communicates with mobile switch center 450, mobile switch center 450 communicates with SMS message center 460, and SMS message center 460 communicates with center 20 is known to those of ordinary skill in the art of wireless networks.

In an alternative preferred embodiment, shown in Fig. 5, center 20 is an SMS message center. In this embodiment authorization communication 30, authentication communication 40, and secure encrypted communication 50 take place over conduit 500. A dialup or other secure connection forms a non-SMS conduit 505 to convey information between SMS message center 20 and credit card center 570.

While the invention has been described in terms of preferred embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.